IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	**No.: 1:22:CR-00123**
v.	**AFFIDAVIT IN SUPPORT OF REQUEST FOR EXTRADITION**
EBUKA RAPHAEL UMETI	

I, Scott W. Nickerson, being duly sworn, hereby depose and state:

1. I am a citizen of the United States and a resident of the State of Virginia.

2. I have been a Special Agent with the Federal Bureau of Investigation (FBI) for over eleven years and am currently assigned to the Washington Field Office. As a Special Agent assigned to a cyber squad, I have received training in, and am authorized to investigate crimes involving computers and computer intrusions, including cyber-enabled fraud scams. I am thus a federal law enforcement officer, as defined by Fed. R. Crim. P. 41(a)(2)(C). Before working at the Washington Field Office, I was a Program Manager at FBI Cyber Headquarters, where I oversaw cyber intrusion investigations at the strategic level.

3. The FBI is one of the agencies within the United States government responsible for the enforcement of federal criminal law. As an agent with FBI, I have received training relating to the investigation of fraud, computer hacking, and the use of computers to facilitate fraud offenses.

4. I am one of the agents assigned to the investigation of the elaborate fraudulent activities of EBUKA RAPHAEL UMETI, also known as "Ebuka Rapheal Umeti," and variations on the online monikers or nicknames "jm.collins," "eternal," and "ebus" (UMETI), and his co-conspirators, including Franklin Ifeanyichukwa Okwonna (Okwonna). I am familiar with the

charges and evidence in this case. The facts set forth in this affidavit are based on my personal knowledge, information supplied to me by other law enforcement personnel, and other sources of information. I am familiar with all aspects of this investigation. The following is a summary of the evidence lawfully obtained during this investigation and does not reflect my entire knowledge of the investigation. In addition, the evidence discussed in this affidavit does not represent all of the evidence collected during the investigation.

BACKGROUND

5. Beginning at least in February 2016, and continuing through at least July 2021, UMETI, Okwonna, and others, including Co-Defendant-3, Co-Conspirator-1, Co-Conspirator-2,[1] conspired and agreed to unlawfully enrich themselves by engaging in business email compromise scams (BEC scams). They gained unauthorized access to the computers of businesses located in the United States and elsewhere, including businesses located in the Eastern District of Virginia, and exploited that access to deceive victims into transferring millions of dollars from their bank accounts. To gain unauthorized access to victim systems, UMETI, Okwonna, and others also routinely damaged victim computers by delivering malicious software or malware.[2]

Overview of Scheme

6. Records and information obtained from numerous victims, the forensic examination of victim devices, and warrants to search dozens of accounts that UMETI,

[1] Co-Conspirator-1 and Co-Conspirator-2 are known by online monikers and identified as unnamed co-conspirators in the Indictment. Co-Defendant-3 is a charged co-defendant whose information is redacted from the Indictment. Premature disclosure of the identifiers for these three individuals would threaten the ability of the United States to identify, locate and arrest them and may lead to their destruction or concealment of evidence.

[2] "Malware" was software designed to disrupt computer operations, gather sensitive information, gain unauthorized access to a computer, or perform other unauthorized actions on a computer.

Okwonna, Co-Defendant-3 and other co-conspirators controlled with email, cloud, and messaging service providers, among other sources, collectively reveal that the co-conspirators pursued a sustained and sophisticated computer hacking and BEC scheme that began at least as early as February 2016.

7. As part of the scheme, UMETI, Okwonna, and their co-conspirators transmitted phishing emails[3] to victim businesses that were made to falsely appear as though they originated from trusted individuals, such as employees at one of the victim's trusted vendors. The defendants and their co-conspirators' phishing attacks often caused the deployment of malicious scripts that gave them unauthorized access to victim computer systems and email accounts. For instance, records obtained pursuant to warrants on the accounts of UMETI, Okwonna, and other co-conspirators at the gaming and messaging platform Discord and the hacking and cybersecurity forum HackForums.net reveal that their phishing emails often attached malicious Microsoft Excel or Word documents—often described as "Macros"[4]—that could then be used to deliver additional malware that provided the defendants and their co-conspirators remote access to the victim devices.

8. The defendants and their co-conspirators then exploited that access to obtain sensitive information needed to deceive victim companies into executing unauthorized wire transfers, including by establishing email processing rules to forward emails automatically from

[3] "Email phishing" or "malware spam" was a fraudulent attempt to install malware by posing as a trustworthy entity in an electronic communication.

[4] A "macro" was an automated input sequence that imitates keystrokes or mouse actions. A macro was typically used to replace a repetitive series of keyboard and mouse actions and used often in spreadsheets and word processing applications, such as Microsoft Excel and Microsoft Word. A "macro malware" was malicious computer code written in the same language used to create the software program, such as Microsoft Word or Excel.

victim employee email accounts to accounts controlled by the defendants and their co-conspirators, without the knowledge or involvement of employees of the victim companies.

9. UMETI, Okwonna, and their co-conspirators then devised, executed, and facilitated BEC scams by impersonating trusted individuals, such as accounts receivable or accounts payable specialists at victim businesses or their corporate partners, in emails and phone calls that fraudulently directed employees of U.S. businesses and banks to wire transfer funds to accounts specified by the defendants and their co-conspirators. The co-conspirators employed several techniques for impersonating trusted individuals, including by sending emails from a trusted individual's compromised account, email spoofing, and creating and using email accounts that closely resembled the individual's account.

UMETI, Okwonna and Others Execute BEC and Computer Hacking Schemes

10. Records lawfully obtained from a domain registrar, Namecheap, the electronic communications service providers Google, Oath Holdings, Inc. (Yahoo), Discord, HackForums, and Dingtone, among others, reveal that UMETI controlled or used a range of online accounts associated with various online monikers to include "jm.collins" and "eternal" that were involved in gaining unauthorized access to victim computer systems and perpetrating and attempting to perpetrate a large volume of BEC scams. Some of the victims impacted by the co-conspirators' scheme include:

Victim Entities	Approximate Actual or Attempted[5] Losses (USD)
An international wholesaler that was located in New York (referred to as "Company A" in Indictment)[6]	$571,274[7]

[5] Victims were sometimes able to recoup the stolen funds after the fraudulent wire transfers.

[6] The victims' names have been withheld to protect their privacy. Consistent with U.S. law, UMETI will be informed of their identities prior to trial.

[7] All references to currency are in U.S. dollars unless otherwise indicated.

A metal supplier located in Texas ("Company B")	$400,385.84
An information services company that was then located in Virginia ("Company C") and a consulting company located in Massachusetts ("Company D")	$109,308
A restaurant chain that was located in Florida ("Company E") and a food services company that was located in Ohio ("Company F").	$482,676.49
A home builder in Texas ("Company G")	$25,426.08
A manufacturing company located in Ohio ("Company H"), a manufacturing company headquartered in Virginia ("Company I"), and an electronics manufacturing company located in Arizona ("Company J")	$1,204,734
A marine supply company located in Virginia ("Company K")	$7,629
An energy equipment and solutions company headquartered in North Carolina ("Company L")	

Scheme to Defraud Companies H, I, and J

11. Records, information, and statements provided by Companies H, I and J, the FBI's forensic analysis of the computer of an accounts receivable and credit management specialist (Employee-1) at Company H, and records from online accounts used by the co-conspirators, collectively reveal that UMETI, Okwonna, and other co-conspirators participated in a BEC scheme to defraud Companies H, I and J from in or around May 2020 through in or around July 2020. As part of the scheme, the co-conspirators transmitted phishing emails and other messages to Employee-1's email account at Company H and gained unauthorized access to the employee's email account and computer. UMETI and his co-conspirators then used information gleaned from the employee's email account to send emails and make phone calls to two of Company H's corporate partners that deceived them into authorizing wire transfers to bank accounts specified by the co-conspirators. Specifically, Company I and Company J were

deceived into initiating bank transfers to the co-conspirators totaling more than $1.1 million. Company I and Company J had intended to transfer the money to Company H.

12. UMETI's central role in the execution of this scheme is demonstrated through evidence developed by the FBI indicating that various online accounts controlled or used by him were involved in both gaining unauthorized access to Employee-1's email account and device, and then defrauding the victims. As an initial matter, a warrant to search a Discord account controlled and used by UMETI (username "eternal101#0438") revealed multiple instances in which he discussed the use of computer infrastructure involved in hacking into Employee-1's email account and deploying malware to the employee's device. For instance, on or about May 4, 2020, UMETI's eternal101#0438 Discord account sent private Discord messages to obtain information needed to access a certain email server. The FBI's forensic analysis of Employee-1's computer, in turn, shows that the actors involved in perpetrating the attack used that same email server on that same day to transmit a phishing email to Employee-1 of Company H that attached a Microsoft Excel spreadsheet called "Remittance Details.xlsm" containing malicious computer code. The FBI's analysis of the code reveals that it was designed to cause unauthorized actions on the employee's computer, including to download a file that would, in turn, download malware from a specified Internet Protocol (IP) address.

13. Further, on or about May 11, 2020, UMETI's eternal101#0438 Discord account discussed hosting the name of a particular file (e-remit.vbs file) on a co-conspirator server that had been downloaded onto Employee-1's computer on the day of the prior phishing attack (May 4, 2020). On or about May 19 and 20, 2020, UMETI's eternal101#0438 Discord account also sent Discord private messages to obtain information needed to access a certain email server and shared that information with a co-conspirator (Co-Conspirator-1 in the Indictment).

Employee-1's device, in turn, shows that an actor involved in the scheme used that email server to transmit a phishing email to Employee-1 of Company H on or about May 26, 2020. This email attached malicious computer code in a Microsoft Excel spreadsheet that was designed to cause unauthorized actions on the computer of Employee-1, including to download a file that would then, in turn, download malware to the employee's computer.

14. In addition, after UMETI gained access to Employee-1's email account, one or more co-conspirators then configured rules within Employee-1's mailbox to hide, move, forward or delete messages automatically without the employee's knowledge. The actor(s) also created filters for segregating emails of interest, including filters tied to the names of certain employees at Company H and other terms that could facilitate future fraud schemes. One of the rules that the actors established was designed to automatically forward the filtered emails to an email address, "jm.collins001@protonmail.com," that the FBI has attributed to UMETI.

15. Records received from Company H show that, on or about May 14, 2020, at least one co-conspirator used the email account of Employee-1 of Company H to send emails to Company J and Company I in which the co-conspirators impersonated Employee-1, and requested that Company J and Company I change the bank account information they used to make payment to Company H. The emails and accompanying email attachments listed telephone numbers that were controlled by an account with a Voice Over Internet Protocol or VoIP account[8] with Dingtone (VoIP Account-1 in Indictment) that has been attributed to UMETI.

[8] "Voice Over Internet Protocol" or "VoIP" was the transmission of voice and multimedia content over an Internet connection. VoIP allowed users to make voice calls from a computer, smartphone, and other mobile devices. A VoIP account could be assigned multiple virtual numbers that could be used for routing voice calls to or from a user's VoIP account.

Notably, records from Dingtone reveal that VoIP Account-1 was registered with an email address, "jm.collins200@icloud.com," that incorporates UMETI's distinctive moniker.

16. In addition, to obscure and delay the detection of the fraud by Company H and its corporate partners as it occurred, one or more co-conspirators sent a series of emails to Company H concerning payment issues in or around May 2020 and in or around June 2020 that falsely purported to be sent from an email address that Company I's parent company in the United Kingdom used to verify transactions. These emails were sent by the co-conspirators from compromised email accounts belonging to third-party corporations that used email servers in the Eastern District of Virginia, including at least three emails that were sent from an email account controlled by a company located in Ohio (Compromised Email Account-1) on or about June 16, 2020 and on or about June 22, 2020. Records received from BitPay, a U.S.-based payment service provider, indicate that the user of UMETI's jm.collins001@protonmail.com account made a payment to Namecheap for a domain registrar account (Namecheap Account-2 in the Indictment) to register a spoofed domain that closely resembled Company I's legitimate domain. Records received from Namecheap and the victim show that the spoofed domain was then used to host an email account used by the co-conspirators to receive replies to the emails sent from the Compromised Email Account-1 on or about June 22, 2020. The spoofed domain was falsely registered with the name "Cassidy Banks" with a mailing address in Hercules, California.

17. The FBI has also uncovered additional evidence tying UMETI's co-conspirators, including Okwonna, to the execution of this scheme. For instance, the FBI's forensic examination of Employee-1's laptop revealed evidence of a friend request from "Ifeanyi Chukwu," which closely mirrors Okwonna's middle name. In relevant part, the text stated "https://www.faceboo.. Ifeanyi Chukwu sent you a friend requ [sic]." Further, another memory

fragment included a phrase that incorporated the online moniker of Co-Conspirator-2 and a reference to a remote monitoring service named "Myq-see." In addition, on or about June 11 and June 12, 2020, at least one co-conspirator transmitted two phishing emails that contained malicious code modified by Co-Defendant-3 to Employee-1 of Company H. The emails attached different Microsoft Excel spreadsheets that both contained code designed to cause unauthorized actions on a recipient computer, including the unauthorized download of a file that, in turn, was coded to download another file named "Attack.jpg" from a specified IP address.

Scheme to Defraud Companies E and F

18. Records and information obtained from Company E and warrants to search email and domain registrar accounts associated with UMETI and his co-conspirators reveal that they executed a BEC scam to defraud Company E in or around July 2019. As part of the scheme, the co-conspirators gained unauthorized access to an employee at Company E (Employee-2) and deceived the company into initiating the transfer of approximately $482,676.49 to a bank account that they specified. Company E had intended to transfer the money to Company F.

19. The role of UMETI and his co-conspirators is demonstrated through multiple ways. As an initial matter, a forensic reported prepared at the request of Company E concluded that the actor(s) first gained unauthorized access to the account of Employee-2's email account through an email phishing attack that included an Excel file macro that was made to appear like a payment notification from Bank of America and then deployed malware suited to maintaining remote access to a victim device. The email phishing attack was transmitted from the email address "cassbanks101@gmail.com," which was used to register above-described Namecheap Account-2. The method and tools associated with this attack are notable because, among other things, records received from Discord and HackForums reveal that UMETI's eternal101#0438

Discord account and HackForums account (username "eternal101") routinely discussed using those techniques and tools. The actions also mimicked the distinctive techniques of UMETI and his actors, including in the scheme to defraud Companies H, I and J. Indeed, as in that instance, a warrant to search a co-conspirator account with Yahoo, "invoice_s231@yahoo.com," revealed that emails were forwarded from Employee-2's email account to that co-conspirator account.

20. In addition, as part of the scheme, in or around July 2019, the actor(s) used Namecheap Account-2 to register two spoof domains and associated email and hosting services that closely mimicked the legitimate domains of Company E and Company F. The actor(s) then used an email address at one of the spoofed domains to impersonate an executive of Company F in emails to Company E that deceived Company E into changing the bank account information that it used to transmit payment to Company F. This activity is notable because a warrant to search yet another account controlled by UMETI, "jm.collins100@yahoo.com," reveals that he contemporaneously sent emails to email address hosted at the spoof domains for Company E and Company F in an apparent effort to test its operation.

Schemes to Defraud Companies A, B, and K

21. The FBI's investigation reveals that accounts attributed to UMETI were directly involved in additional BEC scams that resembled the ones described above, including the schemes to defraud Companies A, B, and K.

22. As an initial matter, records and information provided by Company A indicates that actor(s) gained unauthorized to the email account of an employee at Company A (Employee-3) and used Employee-3's Junk folder to surreptitiously transmit fraudulent emails from the legitimate employee account to corporate partners in January and February 2018. Further, as part of the scheme, the actor(s) impersonated another Company A employee in a series of emails

to Employee-3 and another Company A employee (Employee-4) directing them to fraudulently pay approximately $571,274 owed to a corporate partner to an account specified by the actor(s) on or about January 19, 2018.

23. The role of UMETI and Okwonna in this scheme is demonstrated through multiple ways. First, a warrant to search UMETI's jm.collins100@yahoo.com reveals that it received an email forward from Employee-3's email account of an apparent phishing email that Employee 3 had received. UMETI's jm.collins100@yahoo.com then further forwarded the apparent phishing email to email addresses attributed to Okwonna. Under the circumstances, and in my training and experience, the email forward indicates that UMETI, Okwonna or someone acting in concert with them had gained unauthorized access to the employee's account. The timing of the forward was notable because it took place one day before Company A was deceived into transferring approximately $571,274 to an account specified by the co-conspirators. Second, on or about February 5, 2019, UMETI, using jm.collins100@yahoo.com, appears to have transmitted additional phishing emails to Employee-4 of Company A in an apparent effort to gain further access to that employee account.

24. Similarly, records received from Company B reveal that, in or around 2018, one or more actor(s) gained unauthorized access to an email account of an employee of Company B, and imposed a series of email rules for reading, moving, and forwarding emails within the employee's email inbox that closely mimicked the tactics of the co-conspirators' compromise of Employee-1 at Company H. Notably, the actor(s) set up rules to forward emails that referenced a banking term, error messages, and particular vendors to an account attributed to UMETI (jm.collins002@gmail.com). The employee's email account was then used to send emails that

deceived Company B's vendors into transferring approximately $400,385.84 to accounts specified by the co-conspirators from in or around October through November 2018.

25. In addition, on or about October 6, 2020, UMETI participated in a BEC scam in which an employee of a vendor for Company K was impersonated in emails to Company K that ultimately deceived Company K into transferring approximately $7,629 to a bank account specified by the co-conspirators. Notably, the correspondence listed a telephone number that was controlled by UMETI's VoIP Account-1.

Schemes to Defraud Companies C, D, and G

26. The FBI's investigation reveals that accounts associated with UMETI and his co-conspirators, including Okwonna, have also executed additional BEC schemes in furtherance of the aims of their conspiracy.

27. For instance, records obtained from Company G, Namecheap, and Yahoo collectively reveal that at least one co-conspirator participated in a BEC scam to defraud Company G from in or around September through in or around October 2019. As with other co-conspirator scams, a co-conspirator executed this scheme by gaining unauthorized access to the email account of an employee at Company G and transmitting emails that ultimately deceived Company G into transferring approximately $25,426.08 to a bank account specified by the co-conspirators. Company G had intended to transfer the money to one of its vendors.

28. As part of the scheme, on or about October 4, 2019, a co-conspirator used Namecheap Account-2 to register a spoof domain that mimicked the legitimate domain of Company G. Further, the co-conspirator account "invoice_s231@yahoo.com," which was previously used in the scheme to defraud Company E, transmitted malicious material to Company G email accounts, received internal emails from Company G that were forwarded from

the accounts without authorization, and tested email accounts hosted at the Company G spoof domain on the day (October 4, 2019) it was used to impersonate individuals at Company G.

29. In addition, from March through April 2019, Okwonna participated in a BEC scam that deceived Company C into transferring approximately $109,308 to bank accounts specified by the co-conspirators. Company C had intended to transfer the funds to Company D. As part of the scheme, Okwonna used a different Namecheap account with the username "holmes1010" (Namecheap Account-1 in the Indictment) to register two spoofed domains and host associated email accounts at those domains for the purpose of mimicking the legitimate domain and email accounts of Company D. Okwonna then caused email accounts hosted at the spoofed domains to transmit emails in April 2019 to one or more computers of Company C in the Eastern District of Virginia in which Okwonna impersonated an employee of Company D, and deceived Company C into changing the bank account information it used to transmit payment to Company D.

Scheme to Transmit Malware to Company L

30. Records obtained pursuant to warrants to search co-conspirator Discord and Yahoo accounts, including UMETI's accounts, and the FBI's forensic analysis of a Company L device, collectively show that UMETI and co-conspirators transmitted malware to the computer of a Company L employee (Employee-5), gained unauthorized access to Company L's account, and stole thousands of Employee-5's internal corporate emails.

31. As an initial matter, a warrant to search UMETI's jm.collins100@yahoo.com account revealed that it included two folders that incorporated portions of the names of Employee-5 and Company L. A review of the folders revealed that it contained approximately

22,000 internal corporate emails that were forwarded without authorization from Employee-5's email account from between on or about August 7, 2019 and on or about December 22, 2020.

32. Further, a forensic examination of Employee-5's laptop reveals numerous instances in which compromised servers controlled by the co-conspirators were used to transmit malicious code in 2019 and 2020. For instance, on or about May 19, 2020, Employee-5 received an email that purported to be a payment notification, but attached an Excel file named "Wells Fargo Remittance Advice.xlsm" that was designed to download a file available at a particular uniform resource locator (URL). That is notable because records received from Discord reveal that Co-Conspirator-1 provided this same URL to UMETI through Discord on or about May 10, 2020. In addition, records from UMETI's eternal101#0438 Discord account reveal that he obtained login information for an apparently compromised email server on May 19, 2020, and provided that information to Co-Conspirator-1 on or about May 20, 2020. That server was then used to transmit an apparent phishing email to Employee-5 at Company L on or about May 21, 2020 that purported to be a Citibank payment notification and an executable file. An analysis of that file, in turn, indicates that it caused malicious actions, including contacting a domain, "WorldwideTechSecurity.com," registered by Namecheap Account-2. On or about June 11, 2020, a particular email server was also used to transmit phishing emails to both Company H, as described above, and Company L that purported to be a Wells Fargo payment notification, but contained an Excel attachment that was designed to download a file. The malware attachment listed the nickname of Co-Defendant-=3 as the document's username.

33. The FBI's forensic analysis of Employee-5's laptop also identified a number of malicious files linked to the co-conspirators that remained on the device at the time of imaging.

Additional Evidence of Conspiracy

34. Search warrant returns for email and Discord accounts associated with UMETI and Okwonna, among other accounts, reveal that they have long collaborated on computer hacking and BEC activities, as well as maintained a longstanding personal relationship. Further, as partially highlighted above, Discord chats, emails, domain registrar information, cryptocurrency transactions, and other information show that UMETI and Okwonna have collaborated with additional co-conspirators to include accounts that have been attributed to Co-Conspirator-1, Co-Conspirator-2, and Co-Defendant 3.

35. For instance, while UMETI played an instrumental role in executing the scheme to defraud Companies H, I and J, as detailed above, the forensic examination of Employee-1's laptop showed Okwonna transmitting a Facebook request to Employee-1 and Co-Conspirator-2 accessing a type of surveillance program. Further, Discord chats from May 2020 reveal that Co-Conspirator-2 shared with Co-Conspirator-1 apparent credentials for a website that UMETI then used to host a piece of malware found on Employee-1's computer. Discord chats further show that UMETI sent Co-Conspirator-2 the apparent login credentials for email servers in May 2020 that were used in apparent phishing emails to Company H and Company L in the same month. Similar collaboration is seen in the above-described schemes to defraud Companies A, E, and F.

36. Further, the FBI's investigation has uncovered substantial evidence of the co-conspirators sharing tools and information to further their efforts to gain unauthorized access to victim accounts and systems, and subsequently cause unauthorized wire transfers. As noted above, while BitPay records show that accounts associated with UMETI's "jm.collins" monikers sometimes funded Namecheap Account-2 to further BEC schemes, the account was actually registered with an email address that appears to have been controlled by Co-Conspirator.

Notably, records received from Discord revealed that Co-Conspirator-1's Discord account, which was registered with the registration email address for Namecheap Account-2, routinely corresponded with UMETI's eternal101#0438 Discord account and often appeared to reference UMETI (e.g., through the nickname "Ebus") in conversations with others as if he was a separate person. The chats between UMETI's eternal101#0438 Discord account and Co-Conspirator-1 are notable because they often concerned matters relevant to defrauding corporate victims, including apparent domains, email addresses, usernames, and/or passwords for accessing the computer systems of approximately eight different companies.

37. Warrants to search the Discord accounts attributed to UMETI, Okwonna, and other co-conspirators, including Co-Defendant-3, as well as UMETI's eternal101 account on HackForums, further reveal substantial evidence of the co-conspirators discussing and collaborating on efforts to transmit phishing emails with malware to gain unauthorized access to victim systems. Frequent topics of discussion included (i) efforts to "spam" or "spread" (i.e., to distribute malware) to large groups of victims; (ii) share information about compromised accounts; (iii) purchase malware, such as remote access trojans or RATs, "Remote Control & Surveillance Software" or "Remcos";[9] and other remote surveillance tools, macros for delivering the malware; (iv) obtain crypter services to obfuscate their malware from Co-Defendant-3, among others;[10] and (v) efforts to deploy malware and circumvent anti-virus or email security

[9] Remote Access Trojans," also known as "RATs," were malware that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a computer. A "Remcos" or "Remote Control & Surveillance Software," was a particular type of RAT that could be used to control and monitor computers that used a Microsoft operating system.

[10] A "Crypter" software was a form of malware designed to encrypt, obfuscate, or otherwise manipulate their malware to reduce the chances that their malware would be detected and blocked by antivirus software or other security programs.

systems. Some exemplars of these discussions involving UMETI's eternal101#0438 Discord account and a Discord account attributed to Okwonna (holmes1010#1203) include:

a. In or around February 2020, Okwonna exchanged Discord private messages with Co-Defendant-3 to arrange for Co-Defendant-3 to transfer a crypter tool to Okwonna for a fee.

b. On or about April 20, 2020, UMETI exchanged Discord private messages with Co-Defendant-3 in which he indicated that he received his contact information from the Discord username "Holmes1010" associated with Okwonna. As part of the introductory discussion, UMETI and Co-Defendant-3 discussed UMETI's use of Remcos rats, advised that his tools worked better on certain types of systems, provided instructions on how to use his tools, and cautioned against using Pastebin because "malware hunters are alwyas [sic] there looking for malware." A week later, UMETI confirmed that Co-Defendant-3's crypter was working well and that he was getting "mostly Win10 [machines]."

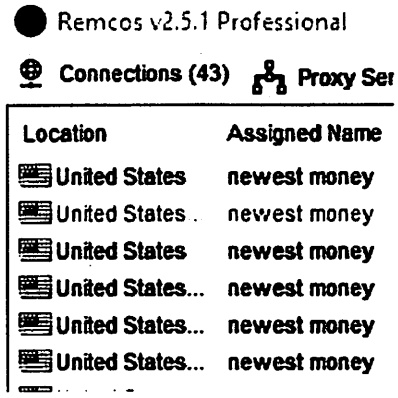
c. In April 2020, UMETI and Co-Defendant-3 exchanged Discord private messages in which Co-Defendant-3 agreed to crypt UMETI's "Remcos" malware for a fee, provided guidance on how to crypt the malware, and described updating the crypter for UMETI in response to the results of a scan through an antivirus software.

d. On or about May 1, 2020, UMETI used Discord to refer Co-Conspirator-1 to Co-Defendant-3 for the purposes of obtaining a crypter tool for "Remcos" malware.

e. On or about June 2, 2020, UMETI and Co-Defendant-3 exchanged Discord private messages in which they agreed for Co-Defendant-3 to provide UMETI with licenses for a "crypter" and a "macro" that were suited to circumvent anti-virus software.

f. On or about July 23, 2020, UMETI and Co-Defendant-3 exchanged Discord private messages to negotiate a transaction in which Co-Defendant-3 agreed to provide UMETI with a private "macro" suited to circumventing a computer's anti-virus security software for a fee, along with an instructional video for using the malware.

g. On or about June 23, 2020, Okwonna sent Discord private messages to Co-Conspirator 2 in which he provided information concerning approximately 28 to 30 compromised devices in the United States to which he had gained unauthorized access through email phishing and the use of "Remcos" malware. Okwonna also sent a screenshot of his apparent "Remcos v.2.5.1." panel that depicts connections to approximately 43 devices, which is partially reflected below:



h. On or about July 23, 2020, UMETI and Co-Defendant-3 exchanged Discord private messages to negotiate a transaction in which Co-Defendant-3 agreed to provide UMETI with a private "macro" suited to circumventing a computer's anti-virus security software for a fee, along with an instructional video for using the malware.

i. In August 2020, Co-Defendant-3 and Okwonna exchanged Discord private messages to negotiate a transaction in which Co-Defendant-3 agreed to renew Okwonna's crypter tool for a fee.

j. In June 2021, UMETI and Co-Defendant-3 exchanged Discord private messages to arrange for UMETI to purchase multiple licenses for Co-Defendant-3's "macro" and "crypter" for UMETI and for others.

38. An examination of chats involving the Discord accounts of UMETI's co-conspirator, including Okwonna, Co-Conspirator-1, and Co-Conspirator-2, reveal many examples of them alluding to his advice and actions as "eternal," "ebuka," or "ebus," including:

a. Between January and August 2020, Okwonna, using holmes1010#1203, and Co-Conspirator-2 exchanged large numbers of private Discord messages about malware tools endorsed or checked by "ebuka" or "ebus" (UMETI), the acquisition of macros, spamming or "shoot[ing]," and efforts to assist each other. Among other things, Okwonna described sending apparent phishing emails to approximately 250 business accounts at a time in April.

b. On or about June 16, 2020, Co-Conspirator-2 exchanged Discord private messages with Co-Defendant-3 in which he explained how he was spamming or spreading malware to an email list. In relevant part, Co-Conspirator-2 explained that "***7 of us spreading to the same people.. and most of them use you.. [moniker of Co-Conspirator-1], holmes [Okwonna], eternal [UMETI].***" (Emphasis added). Co-Defendant-3 then said, "***yeah i know those dudes***." (Emphasis added).

c. Between in or around May and August 2020, Co-Conspirator-1 and Co-Conspirator-2 exchanged Discord messages in which they discussed spamming victims, macros, and using smtp servers and RATs, such as Remcos. As part of the discussions, they often referenced software or contacts that UMETI had approved or recommended (e.g., as "ebuka" or "ebus"). For instance, on or about May 6, 2020, the co-conspirators discuss sending "boxes"—

i.e., compromised email accounts—to "ebus," and they agree to "bomb" the "AR/AP"—i.e., account receivable/account payable—contacts from the compromised accounts.

39. The FBI's investigation has also identified several additional sources of evidence that highlight the close collaboration amongst UMETI, Okwonna, and others in furtherance of the scheme include. For instance, records received from BitPay and the FBI's analysis of the blockchain[11] reveal evidence that both Namecheap Account-2 (used in the schemes targeting Companies E, F, G, H, I, and J) and Namecheap Account-1 (used in the scheme targeting Companies C and D) were financed through Bitcoin addresses that may be traced back to a common wallet in 2019.

40. The FBI's investigation also indicates that Okwonna controlled a Google account associated with the email address "hawlalalam.ali@gmail.com" to harvest credentials, conduct other BEC-related activity, and correspond with other co-conspirators, including UMETI. For instance, records obtained through warrants on UMETI's jm.collins100@yahoo.com account and Okwonna's hawlalalam.ali@gmail.com account, respectively, show that both accounts stored historic emails with the common subject "FWESHBOIZ INC!" that listed apparent username, password, and IP address information that appeared suited to gaining unauthorized access to victim accounts. Based on the volume of emails, the common subject, and my training and experience, it appears that, at different points, both UMETI and Okwonna shared a common source for harvesting credentials for accessing victim accounts or computers.

41. Records obtained pursuant to email warrants further showed that, between on or about February 29, 2016 through on or about November 1, 2017, Okwonna's

[11] The blockchain is a publicly available digital ledger that tracks cryptocurrency transactions. Cryptocurrency transactions are processed in blocks, which are then added to the chain, hence the term blockchain.

hawlalalam.ali@gmail.com account sent emails to accounts controlled by UMETI, including jm.collins100@yahoo.com, that, in my training and experience, appear to contain templates for fraud or email phishing scams.

42. Additional accounts attributed to UMETI and Okwonna reveal substantial evidence of their longstanding personal relationship, including evidence of the two traveling and posing for photographs together, as well as sharing sensitive personal information. Indeed, an iCloud account attributed to Okwonna, "franklin_franklin@icloud.com," contained photographs of passports and visas for both UMETI and Okwonna. In addition, another Google account attributed to UMETI, "eternal1502@gmail.com," contained bank statements for "Ebuka Raphael Umeti" from the Guaranty Trust Bank PLC that showed multiple bank transfers to Okwonna, including two transfers to Okwonna in or around May 2020 – e.g., near the time of the BEC scheme to defraud Companies H, I and J.

Identification of UMETI

43. As further detailed below, the FBI's investigation indicates that UMETI committed the acts attributed to him above through Namecheap Account-2, VoIP Account-1, and a large number of additional accounts associated with his distinctive "jm.collins" and "eternal" online monikers. These accounts contained some evidence of UMETI's identity and ultimately led to the identification of two Google accounts, eternal1502@gmail.com and ebuka1502@gmail.com, that provided strong confirmation of UMETI's real identity.

UMETI's Distinctive Use of "Jm.Collins" and "Eternal" Monikers

44. Based on my training and experience, I understand that cybercriminals often use common username or variations on a common username to build and maintain their reputations amongst other hackers. I am further aware that individuals engaged in criminal cyber activity

commonly create multiple email accounts to better disguise their activity. These accounts are often used to register online accounts on websites and other platforms associated with criminal activity, retain control over the online accounts in the event access to it is compromised or otherwise interrupted (e.g., forgotten password), receive notifications regarding the use of the online accounts, and correspond with co-conspirators. Due to the intended use of such originating email accounts, the offender generally maintains sole control over the account or utilizes the account with others engaged in the same or similar misconduct.

45. Here, records lawfully obtained from Namcheap, Dingtone, Google, Yahoo, HackForums, Discord, and GitHub[12] indicate that a common actor—UMETI—used a range of accounts that are linked together through a number of ways, including the shared associations with the distinctive "jm.collins" and "eternal" online monikers. These accounts include Namecheap Account-2, VoIP Account-1, jm.collins100@yahoo.com, jm.collins001@protonmail.com, jm.collins200@icloud.com, and jm.collins002@gmail.com, the eternal101 HackForums account, the eternal101#0438 Discord account, and a GitHub account associated with the username "eternal1502."

46. As an initial matter, each of these accounts either employed the distinctive "jm.collins" moniker or can been directly tied to an account with the "jm.collins" moniker. For instance, records from Namecheap and BitPay reveal that the user of the email addresses jm.collins100@yahoo.com and jm.collins001@protonmail.com paid for domains registered through Namecheap Account-2 in 2019 and 2020, including the spoof domain that was used in the scheme to defraud Companies H, I and J. VoIP account-1 was registered with jm.collins200@icloud.com. The recovery email address for jm.collins100@yahoo.com was

[12] Github is a U.S.-based Internet hosting service for software development.

jm.collins001@protonmail.com, and jm.collins100@yahoo.com was the registration email address for the eternal101 HackForums account, the eternal101#0438 Discord account, and the eternal1502 GitHub account.[13]

47. The accounts also included additional substantive links. For instance, records received from Yahoo concerning the jm.collins100@yahoo.com account revealed that, on or about July 11, 2019, the jm.collins100@yahoo.com account sent an email to jm.collins002@gmail.com in an apparent effort to test a spoof domain for Company E. As detailed above, that email was notable because the Company E spoof domain was registered by Namecheap Account-2 and used in the BEC scam to defraud Company E. Further, in or around February 2019, the jm.collins100@yahoo.com account transmitted apparent phishing emails to an employee of Company A that listed jm.collins002@gmail.com as a recipient.

48. The accounts also discussed common techniques and activities. For instance, both the eternal101 Hack Forums and eternal101#0438 Discord accounts routinely discussed the acquisition and use of certain classes of malicious computer tools. The eternal101 Hack Forums account and eternal1502 GitHub account both posted about the topic of a technique known as "VBS obfuscation" in the timeframe of on or about June 16 and 17, 2016.

49. Login records from these various accounts further indicate that they appear to be controlled by a common actor. For instance, on or about August 19, 2020 and October 28, 2020, Namecheap Account-2 and the jm.collins100@yahoo.com account were both accessed from a common IP address. The same IP address also accessed both Namecheap Account-2 and the

[13] In my training and experience, a recovery or registration email provides a means for retaining control over a primary account in the event that access to it is compromised or otherwise interrupted (e.g., password).

eternal101 Hack Forums account on or about March 12, 2020.[14] Similarly, login data reveals that the eternal101 HackForums account and the eternal1502GitHub account were both accessed from another common IP address on or about June 16, 2016.

50. The Namecheap Account-2, eternal1502 GitHub account, and co-conspirator Discord accounts also contained evidence of UMETI's identity. Notably, records received from Namecheap concerning Namecheap Account-2 revealed a log file titled "awstats112020.achremittanceservices.com.txt." This log file contained, among other data, error notifications concerning the domain achremittanceservices.com that listed entries that referenced, among other names, UMETI's first name "Ebuka," a variation on UMETI's middle name "Rapheal,"[15] and the "collins" moniker. Some of the entries include:

/ADP/mod_ebuka/
/Excel/ebuka/
/Excel/mod_ebuka/
/ADP/ebuka/
/Excel/Ebuka/
/ADP/Ebuka/
/ADP/rapheal/
/Excel/rapheal/
/Excel/~collinsw/
/ADP/collins/
/ADP/collins/admin.php
/Excel/collins/
/ADP/~collinsw/
/Excel/collins/admin.php

[14] In my training and experience, logins into multiple accounts from a common IP address around the same dates and times likely indicates that they were accessed from a common device or network.

[15] The word "Rapheal" transposes the "e" and "a" from UMETI's formal middle name "Rapheal." However, records from the eternal1502@gmail.com revealed that UMETI used the names "Raphael" and "Rapheal" interchangeably.

51. In addition, within one of the eternal1502 GitHub account's posts on or about June 20, 2016, eternal1502 provided a screenshot of a computer terminal screen that displayed a Windows command prompt with the filepath "C:\Users\Raph>". As noted above, UMETI's middle name is Raphael.

52. Further, as noted above, Discord private messages sent by Okwonna and Co-Conspirator-1 in 2020 sometimes referenced malware or computer-related recommendations or endorsements provided by "ebuka." As noted above, UMETI's first name is "Ebuka."

Additional Evidence of UMETI's Identity

53. The FBI's analysis of these accounts, including the eternal1502 GitHub account, ultimately led to the identification of the eternal1502@gmail.com and ebuka1502@gmail.com accounts. Records lawfully obtained from Google concerning these accounts revealed substantial evidence of UMETI's identity. For instance, a Google payments account in UMETI's full name of "Ebuka Raphael Umeti" was listed as a related service for the eternal1502@gmail.com account. The account also showed multiple emails that referenced the UMETI identity. For example, on or about November 20, 2020, the eternal1502@gmail.com account sent an email that attached a photograph of a college degree that was awarded to "Umeti Ebuka Raphael" from Anambra State University, in Uli Ihiala, Nigeria on or about February 29, 2012. Further, on or about May 8, 2019, the eternal1502@gmail.com sent itself an email that attached an application for a Schengen Visa that listed the full name of Ebuka Raphael UMETI, date of birth "15/02/1989", place of birth "Ihiala, Nigeria." The birthdate is notable because, among other things, its date-month formulation (15/02) corresponds to the "1502" moniker used by UMETI, including the eternal1502 GitHub account, eternal1502@gmail.com account, and ebuka1502@gmail.com account.

54. The eternal1502@gmail.com Google account and UMETI's identification information tie UMETI directly to accounts involved in the above-described criminal activity. For instance, the eternal1502@gmail.com account and VoIP account-1 were both accessed from a common IP address (41.190.14.204) within mere minutes of each other on or about September 4, 2020.

55. A warrant to search an account (franklin_franklin@icloud.com) of one of UMETI's co-conspirators, Okwonna, also revealed a photograph of UMETI's Nigerian passport that contained his name and birth information. As noted below, UMETI was in possession of the same passport at the time of his arrest at the Jomo Kenyatta International Airport.

Risk of Flight

56. The FBI's investigation indicates that UMETI is a significant flight risk. As the above-described BEC scams highlight, UMETI has a long history of possessing stolen identity information and a demonstrated capacity to effectively present himself as someone else. Accordingly, it is reasonable to expect that UMETI would attempt to flee under fake or stolen identities. UMETI also has the means to travel. Indeed, the FBI has received information indicating that UMETI has routinely traveled abroad in recent years, including to the Maldives, Zanzibar in Tanzania, and Qatar, among other places. Accounts attributed to UMETI and Okwonna also contained evidence of visa applications to authorize travel to France, Germany, and the United Arab Emirates. In my experience, the seriousness of the penalties that UMETI could face, if convicted, also creates a strong incentive to flee.

IDENTIFICATIONAND LOCATION INFORMATION

57. EBUKA RAPHAEL UMETI, also known as Ebuka Rapheal Umeti, and variations on the online monikers or nicknames "jm.collins" "eternal," and "ebus," is a citizen of Nigerian born on February 15, 1989 in Ihiala, Nigeria. He is described as a black male with

black hair and brown eyes. He holds a Nigerian passport, number A10463547, issued on April 25, 2019. He was arrested on June 11, 2023 at the Jomo Kenyatta International Airport and has been detained pending extradition proceedings.

58. Attached to this affidavit as **Attachment 1** is a copy of UMETI's passport, obtained from him following his arrest in Kenya. Julius F. Nutter, FBI Assistant Legal Attaché, U.S. Embassy Nairobi, to Kenya, was present at UMETI's arrest and can identify this photograph as being that of UMETI.

SCOTT W. NICKERSON
FEDERAL BUREAU OF INVESTIGATION

SWORN AND SUBSCRIBED BEFORE ME
THIS 20TH DAY OF JUNE, 2023.

HON. WILLIAM E. FITZPATRICK
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF VIRGINIA

ATTACHMENT 1

Photograph of Ebuka Rapael UMETI